REMARKS

Claims 1-4 and 6-8 stand rejected under 35 U.S.C 102 (e) as being allegedly anticipated by Hazama (6,089,460). Claim 5 stands rejected under U.S.C 35 103 as allegedly being obvious over Hazama in view of Tanaka (4,924,075).

The Applicant respectfully traverses these rejections for the reasons set out below.

To anticipate a claim, the reference must teach every element of the claim. "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

The essence of the invention has been further clarified by the addition of the phrase 'having the same functionality' to independent claims 1, 6 and 8. In this way, it is made clear that the invention lays claim to a security system, set of secure devices and method for manufacturing a secure device, wherein the chips in each secure device, or group of secure devices, performs the same logic, but has a different layout. The basis for this amendment can be found, amongst others, in the specification on page 5, lines 22-23.

It is submitted that the subject matter of the independent claims is not disclosed in Hazama. Hazama does not teach a number of secure devices with logic circuitry with the same functionality, wherein in at least a part of said secure devices, the chip of a secure device is provided with a unique chip layout. Thus, two different chips may have different layouts but the same functionality.

Hazama teaches an embodiment of a semiconductor security device with a security protection function, in which the layout of each chip is unique but the logic circuitry of the chip does not have the same functionality. In this embodiment (described in column 8, lines 35-40),

4

codes are allocated to a plurality of programs for programming the FPGA 20. When the FPGA is programmed, the FPGA 20 is programmed in accordance with a program selected from a plurality of the programs. In this case, the program code is also stored. To access the programmed FPGA, the stored program code is output to an external unit via CPU 30. In other words, Hazama clearly teaches away from the present invention in disclosing this embodiment, since it is clear the any device checking secure devices needs to know the logic programmed into that particular device in order to access it. The functionality, the program in the FPGA 20 which calculates structural data on the basis of logical data (column 7, line 52-53), thus clearly differs according to the code used to program the FPGA.

In one embodiment, Hazama teaches that each secure device is programmed using the same code. Ciphering and deciphering programs (used to translate structural to logical addresses and vice versa) are written in the FPGA by the data supplied from a CPU in the secure device (column 6, lines 52- 53). Hazama does not teach that the ciphering and deciphering programs are written by data supplied from the CPU that varies the hardware layout of the logic circuitry from one secure device or set of secure devices to the other.

The first embodiment taught by Hazama has the distinct disadvantage that the code necessary to read and write to the secure device must be made available to any device wishing to check it. On the one hand this adds extra complexity to the system, on the other hand this affords hackers an opportunity for tricking the secure device into transferring the stored program code to an external unit via the CPU 30.

The second embodiment taught by Hazama has the disadvantages already discussed in the specification of the present application. Once one smart card programmed according to a certain program has been analyzed to identify appropriate probe points to access the data contained in the chip - more precisely in this case, the logic to translate structural memory addresses to logical addresses - any second attack on a further smart card is relatively easy.

It is thus submitted that claims 1, 6 and 8 of the present invention, that include the limitation of a chips "having the same functionality", but being "provided with a unique layout" per secure device or group of secure devices, is not taught or suggested by Hazama. Accordingly, the present invention as claimed in claims 1, 6 and 8 is novel in view of Hazama. As claims 2-5, 7 and 9-10 are dependent upon allowable claims 1, 6 and 8 respectively, they are also allowable.

Claim 5 stands rejected under U.S.C 35 103 as allegedly being obvious over Hazama in view of Tanaka (4,924,075). However, claim 5 is indirectly dependent upon claim 1, which is submitted to be allowable and, accordingly, claim 5 is also allowable.

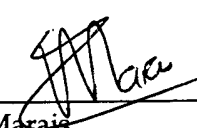In view of the above, allowance of the presently pending claims is courteously solicited.

It should furthermore be noted that the above amendments to the claims have not been made within view to overcoming any prior art of which the Applicants are aware, or that has been cited in the present Office Action. The above amendments have been made with a view to modifying the form of the claims.

If there are any additional charges, please charge Deposit Account No. 02-2666. If a telephone interview would in any way expedite the prosecution of the present application, the Examiner is invited to contact André Marais at (408) 947-8200.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: _____ 08/22/, 2002

André L. Marais
Reg. No. 48,095

12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026
(408) 947-8200

<u>IN THE CLAIMS:</u>

Please amend the claims as follows:

1.   (Amended) Security system for checking authorization, the system including a number of secure devices, each of said secure devices comprising a chip with logic circuitry, having a function in providing authorization to the security system, characterized in that in at least a part of said secure devices, the chip of a secure device is provided with a unique chip layout, <u>having the same functionality</u>.

2.   (Unamended) Security system according to claim 1, wherein at least said logic circuitry of the chips of said part of the secure devices is implemented in Field Programmable Gate Array FPGA technology, wherein the layout is programmed in the FPGA circuitry in at least one of a volatile and a non-volatile manner.

3.   (Unamended) Security system according to claim 2, wherein the logic circuitry of each secure device chip is provided in a secure cell of the chip.

4.   (Unamended) Security system according to claim 1, wherein the complete secure device ship is implemented in FPGA technology, wherein the layout is programmed in the chip in at least one of a volatile and a non-volatile manner.

5.   (Unamended) Security system according to claim 2 wherein at least one of the logic circuitry and the entire chip is made as a volatile programmable FPGA, wherein the FPGA program is stored in a battery powered RAM.

6.   (Amended) A set of secure devices for a security system according to claim 1, wherein each of said secure devices comprises a chip with logic circuitry having a function in providing authorization to the holder of a secure device, wherein in at least a part of said secure devices, the chip of each secure device is provided with a unique chip layout, <u>having the same functionality</u>.

7.   (Unamended) A set according to claim 6, wherein at least said logic circuitry of the chips of said part of the secure devices is implemented in FPGA technology, wherein the layout is programmed in the FPGA circuitry in at least one of a volatile and a non-volatile manner.

8.   (Amended) Method for manufacturing a secure device for a security system according to claim 1, wherein secure devices with a chip are used, said chips having logic

7

circuitry having a function in providing authorization to the security system, wherein in at least a part of said secure devices, the chip of a secure device is provided with a unique chip layout, <u>having the same functionality</u>.

9. (Unamended) Method according to claim 8, wherein chips with logic circuitry in FPGA technology are use, said method comprising programming a unique information in the logic circuitry utilizing a synthesis tool and a layout tool, wherein for each secure device of said part of secure devices, a variation factor is introduced in at least one of the synthesis tool and the layout tool, thereby providing a unique circuit layout.

10. (Unamended) Method according to claim 9, wherein the synthesis tool is provided with input information compiled from a high level language code, wherein a variation factor is introduced in at least one of the compilation step of the high level language code, the synthesis tool and the layout tool.